

# Probabilistic Computation

Lecture 13  
BPP vs. PH

# Recap

- Probabilistic computation
- NTM (on "random certificates") for  $L$ :

•  $\Pr[M(x)=\text{yes}]$ : 

• PTM for  $L$ :  $\Pr[\text{yes}]$ : 

• BPTM for  $L$ :  $\Pr[\text{yes}]$ : 

• RTM for  $L$ :  $\Pr[\text{yes}]$ : 

# Recap

- PP, RP, co-RP, BPP
  - PP too powerful:  $NP \subseteq PP$
  - RP, BPP, with bounded gap
    - Gap can be boosted from  $1/\text{poly}$  to  $1-1/\text{exp}$
    - A realistic/useful computational model
- Today:
  - $NP \not\subseteq BPP$ , unless PH collapses
  - $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

# BPP vs. NP

- Can randomized algorithms efficiently decide all NP problems?
  - **Unlikely:**  $NP \subseteq BPP \Rightarrow PH = \Sigma_2^P$
  - Will show  **$BPP \subseteq P/poly$** 
    - Then  $NP \subseteq BPP \Rightarrow NP \subseteq P/poly$ 
      - $\Rightarrow PH = \Sigma_2^P$

# BPP $\subseteq$ P/poly

- If error probability is sufficiently small, will show there should be at least one random tape which works for all  $2^n$  inputs of length  $n$ 
  - Then, can give that random tape as advice
- One such random tape if average (over  $x$ ) error probability is less than  $2^{-n}$ 
  - BPP: can make worst error probability  $< 2^{-n}$

$r \backslash x$						
	✓	✗	✗	✓	✓	✓
	✓	✓	✓	✓	✓	✗
	✓	✓	✓	✓	✓	✓
	✓	✓	✗	✓	✓	✓
	✓	✓	✓	✓	✗	✓
	✗	✗	✓	✓	✓	✓
	✗	✓	✓	✓	✓	✓
	✓	✓	✓	✗	✓	✓
	✓	✓	✓	✓	✗	✓
	✓	✓	✓	✗	✓	✓
	✓	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✗
	✓	✓	✓	✓	✓	✓

# BPP vs. PH

- $BPP \subseteq \Sigma_2^P$

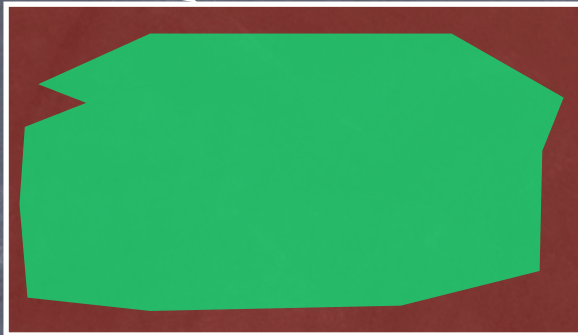
- So  $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

$$\text{BPP} \subseteq \Sigma_2^P$$

- $x \in L$ : "for almost all"  $r$ ,  $M(x,r)=\text{yes}$
- $x \notin L$ :  $M(x,r)=\text{yes}$  for very few  $r$
- $L = \{ x \mid \text{for almost all } r, M(x,r)=\text{yes} \}$ 
  - If it were "for all", in coNP
  - $L = \{ x \mid \exists \text{ a small set of "shifts" } P, \forall r, \text{ for some } r' \in P^{-1}(r), M(x,r')=\text{yes} \}$ 
    - Note:  $P^{-1}(r)$  is a small set of shifts, so can go through all of them in polynomial time

$$\text{BPP} \subseteq \Sigma_2^P$$

$$x \in L: |\text{Yes}_x| > (1 - 2^{-n}) 2^m$$



$$x \notin L: |\text{Yes}_x| < 2^{-n} 2^m$$



Space of random tapes =  $\{0,1\}^m$

$$\text{Yes}_x = \{r \mid M(x,r) = \text{yes}\}$$

- $x \in L$ : Will show that there exist a small set of shifts of  $\text{Yes}_x$  that cover all  $r$ 's
- $x \notin L$ :  $\text{Yes}_x$  very small, so its few shifts cover only a small region

$$\text{BPP} \subseteq \Sigma_2^P$$

- “A small set of shifts”:  $P = \{u_1, u_2, \dots, u_k\}$ 
  - $P(r) = \{r \oplus u_1, r \oplus u_2, \dots, r \oplus u_k\}$  where  $r, u_i$  are  $m$ -bit strings, and  $k$  is “small” (poly( $n$ ))
- For each  $x \in L$ , does there exist a  $P$  s.t.  $P(\text{Yes}_x) := \bigcup_{r \in \text{Yes}(x)} P(r) = \{0,1\}^m$ ?
  - Yes! Can find a  $P$  s.t. for all large  $S$  (like  $\text{Yes}_x$ )  $P(S) = \{0,1\}^m$ 
    - In fact, most  $P$  work (if  $k$  big enough)!

$$\text{BPP} \subseteq \Sigma_2^P$$

- Probabilistic Method (finding hay in haystack)
  - To prove  $\exists P$  with some property
  - Define a probability distribution over all candidate  $P$ 's and prove that the property holds with positive probability (often even close to one)
    - Distribution s.t. easy to prove positive probability of property holding

$$\text{BPP} \subseteq \Sigma_2^P$$

- Probabilistic method to find  $P = \{u_1, u_2, \dots, u_k\}$ , s.t. for all large  $S$ ,  $P(S) = \{0,1\}^m$ 
  - Distribution over  $P$ 's: randomized experiment to generate  $P$ 
    - Pick each  $u_i$  independently, and uniformly at random from  $\{0,1\}^m$
- $\Pr_{(\text{over } P)}[P(S) \neq \{0,1\}^m] = \Pr_{(\text{over } P)}[\exists z \ z \notin P(S)]$ 

$$\leq \sum_z \Pr_{(\text{over } P)}[z \notin P(S)] = \sum_z \Pr_{(\text{over } u_1..u_k)}[\forall i \ z \oplus u_i \notin S]$$

$$= \sum_z \prod_i \Pr_{(\text{over } u_i)}[z \oplus u_i \notin S] = \sum_z \prod_i (|S^c|/2^m) < \sum_z \prod_i 2^{-n}$$

$$= 2^m \cdot (2^{-n})^k = 1$$
- So (with  $|S| > (1-2^{-n})2^m$  and  $k=m/n$ ),  $\exists P, P(S) = \{0,1\}^m$

$$\text{BPP} \subseteq \Sigma_2^P$$

$$x \in L: |\text{Yes}_x| > (1 - 2^{-n}) 2^m$$



$$x \notin L: |\text{Yes}_x| < 2^{-n} 2^m$$



Space of random strings =  $\{0,1\}^m$

$$\text{Yes}_x = \{r \mid M(x,r) = \text{yes}\}$$

- For each  $x \in L$ ,  $\exists P$  (of size  $k = m/n$ ) s.t.  $P(\text{Yes}_x) = \{0,1\}^m$
- For each  $x \notin L$ ,  $P(\text{Yes}_x) \subsetneq \{0,1\}^m$ 
  - $|P(\text{Yes}_x)| \leq k |\text{Yes}_x| = (m/n) 2^{-n} 2^m < 2^m$
- $L = \{x \mid \exists P \forall r \text{ for some } r' \in P^{-1}(r) M(x,r') = \text{yes}\}$

# BPP-Complete Problem?

- Not known!

- Usual attempt:  $L = \{ (M, x, 1^t) \mid M(x) = \text{yes in time } t \text{ with probability } > 2/3 \}$

- Is indeed BPP-Hard

- But in BPP?

- Just run  $M(x)$  for  $t$  steps and accept if it accepts?

- If  $(M, x, 1^t)$  in  $L$ , we will indeed accept with prob.  $> 2/3$

- But  $M$  may not have a bounded gap. Then, if  $(M, x, 1^t)$  not in  $L$ , we may accept with prob. very close to  $2/3$ .

# BPTIME-Hierarchy Theorem?

- $\text{BPTIME}(n) \subsetneq \text{BPTIME}(n^{100})$ ?
- Not known!
  - But is true for  $\text{BPTIME}(T)/1$

# Today

- Probabilistic computation
- $BPP \subseteq P/poly$  (so if  $NP \subseteq BPP$ , then  $PH = \Sigma_2^P$ )
- $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$
- Coming up
  - Basic randomized algorithmic techniques
  - Saving on randomness